This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-13 (cancelled).

14 (currently amended). A system for providing a content item, said system comprising:

a plurality of download servers, wherein each download server receives a request for said content item, said request comprising encrypted data that represents a public key associated with a user from whom said request is received and an identification of said content item, said request having been generated at a first server with which said user has previously engaged in a transaction to purchase said content item, said encrypted data having been encrypted with a first key, each of said download servers having:

a cache which stores said content item; and

a first object which receives a first message to invalidate said content item in said cache and which invalidates said content item in said cache in response to receipt of said first message; and

a fulfillment server having:

a content store which stores said content item; and

a first database which stores information relating to said content item; and

a second object which receives a notification that said information in said first database has been updated or deleted, and which generates, in response to said notification, said first message for dispatch to said plurality of download servers,
said first server being separate from said plurality of download servers and from said fulfillment server, said first key being known to said first server and to said plurality of download servers but not to said user, each of said plurality of download servers comprising logic that applies said first key to said encrypted data to retrieve said identification of said content item and said first key, and that uses said public key to encrypt a second key that is used to decrypt said content item, said content item being provided to said user in a form

encrypted with said second key and including said second key in a form encrypted by said public key.

15 (original). The system of claim 14, wherein said fulfillment server further includes a second database which stores a log of events occurring on said plurality of download servers, wherein each of said plurality of download servers generates a second message for dispatch to said fulfillment server in response to said events, and wherein said second object receives said second message and logs said events in said second database.

16 (currently amended). The system of claim 14, wherein said events include the downloading of said content item to said user who is a purchaser of said content item, said user having engaged in a purchase transaction with said first server, said first server including functionality to determine whether to generate said request or not to generate said request depending on whether the user has completed said purchase transaction.

17 (original). The system of claim 14, wherein said content item is sold by a retailer for download by one of said plurality of download servers, and wherein said first database further stores information relating to said retailer.

18 (original). The system of claim 17, wherein said plurality of download servers is hosted by said retailer.

19 (currently amended). The system of claim 14, wherein ~~said download servers provide said content item for durable storage on one or more computing devices associated with consumers of said content item~~ said user has previously obtained said public key by engaging in a transaction with a second server that distributes and installs public keys and their corresponding private keys on machines, said second server comprising logic that performs acts comprising:

maintaining an association between said user, said public key, and a private key associated with said public key;

receiving a request to install said public key and said private key on a

machine;

authenticating the user from whom the request is received as a condition to installing said public key and said private key on said machine;

determining that a limit on the number of machines on which said user's public key and private key may be installed has not been exceeded as a further condition to installing said public key and said private key on said machine; and

installing said public key and said private key on said machine by delivering a certificate that includes said public key and said private key with at least said private key being encrypted by a platform public key that is associated with, and relatively unique to, said machine.

20 (original). The system of claim 14, wherein each of said first and second object is an instance of an MSMQ independent client.

21 (currently amended). A computer-implemented method of using a plurality of servers to distribute a content item, said method comprising the acts of:

receiving, at a first of said plurality of servers from a first computing device, a request for said content item, said first server having a first cache;

determining that no valid copy of said content item exists in said first cache;

obtaining said content item at said first server from a content store;

providing said content item to said first computing device;

storing said content item in said first cache;

receiving, at a fulfillment server, a change to an attribute of said content item, said attribute being stored at said fulfillment server;

said fulfillment server sending a notification to said plurality of servers in response to said change; and

said first server invalidating said copy of said content item in said first cache in response to said notification,

each of said plurality of servers comprising logic that performs acts comprising:

receiving, from a user, a request to provide said content item to a user, said request comprising a public key associated with said user and an identification of said

content item, said public key and identification being in an form encrypted by a first key that is known to each of said plurality of servers and to a first server at which said request is generated but that is not known to said user, said public key being installed by an activation server on a plurality of machines associated with said user.

22 (previously presented). The computer-implemented method of claim 21, wherein said act of sending a notification comprises using a store-and-forward messaging facility.

23 (previously presented). The computer-implemented method of claim 21, wherein said change comprises a change in a physical location of said content item.

24 (currently amended). The computer-implemented method of claim 21, ~~wherein said change comprises a change in a level of protection to be applied to said content item~~ wherein said activation server enforces a limit as to the number of machines associated with said user on which said public key may be installed, said limit being initially set to a first number, and said limit being increasable beyond said first number if a standard that governs the increase in said limit has been met, said public key being installed on each of said users machines along with a private key corresponding to said public key in a manner so as to make an installation of said private key unusable if said installation of said private key is copied to a machine other than a machine on which said private key has been installed by said activation server.

25 (previously presented). The computer-implemented method of claim 21, wherein said content item comprises:

encrypted content; and

a first cryptographic key which decrypts said encrypted content.

26 (previously presented). The computer-implemented method of claim 25, wherein said content item further comprises meta-data, wherein said first cryptographic key is sealed with said meta-data.

27 (previously presented). The computer-implemented method of claim 25, wherein said encrypted content is stored in said cache separately from said first cryptographic key.

28 (previously presented). The computer-implemented method of claim 21, wherein said change comprises a change in the meta-data of said content item.

29-36 (cancelled).

37 (currently amended). A computer-readable medium encoded with computer-executable instructions to perform a method of using a plurality of servers to distribute a content item, the method comprising:

receiving, at a first of said plurality of servers from a first computing device, a request for said content item, said request being received from a user and having been generated at a server remote from said user, said request comprising an identification of a content item and a public key associated with said user, said request being in a form encrypted with a first cryptographic key that is known to said plurality of servers and to said server remote from said user, but that is not known to said user, said content item being encrypted in a form that is decryptable with said first cryptographic key, said first cryptographic key being included in said content item in a from encrypted with said public key, said first server having a first cache;

determining that no valid copy of said content item exists in said first cache;

obtaining said content item at said first server from a content store;

providing said content item to said first computing device;

storing said content item in said first cache;

receiving, at a fulfillment server, a change to an attribute of said content item, said attribute being stored at said fulfillment server;

said fulfillment server sending a notification to said plurality of servers in response to said change; and

said first server invalidating said copy of said content item in said first cache in response to said notification.

38 (previously presented). The computer-readable medium of claim 37, wherein said act of sending a notification comprises using a store-and-forward messaging facility.

39 (previously presented). The computer-readable medium of claim 37, wherein said change comprises a change in a physical location of said content item.

40 (previously presented). The computer-readable medium of claim 37, wherein said change comprises a change in a level of protection to be applied to said content item.

41 (currently amended). The computer-readable medium of claim 37, wherein said content item comprises:

encrypted content; and

[[a]] said first cryptographic key which decrypts said encrypted content.

42 (previously presented). The computer-readable medium of claim 41, wherein said content item further comprises meta-data, wherein said first cryptographic key is sealed with said meta-data.

43 (previously presented). The computer-readable medium of claim 41, wherein said encrypted content is stored in said cache separately from said first cryptographic key.

44 (previously presented). The computer-readable medium of claim 37, wherein said change comprises a change in the meta-data of said content item.